INTERNATIONAL STANDARD

ISO/IEC 11586-6

First edition
1997-04-01

Information technology — Open Systems Interconnection — Generic upper layers security: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) proforma

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Sécurité générique pour les couches hautes: Proforme de déclaration de conformité pour la mise en œuvre du protocole (PICS) de la syntaxe de transfert de protection

Reference number
ISO/IEC 11586-6:1997(E)

Contents

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 11586-6 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.835.

ISO/IEC 11586 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — Generic upper layers security*:

— *Part 1: Overview, models and notation*

— *Part 2: Security Exchange Service Element (SESE) service definition*

— *Part 3: Security Exchange Service Element (SESE) protocol specification*

— *Part 4: Protecting transfer syntax specification*

— *Part 5: Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma*

— *Part 6: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) Proforma*

Annex A forms an integral part of this part of ISO/IEC 11586.

Introduction

This Recommendation | International Standard forms part of a series of Recommendations | International Standards that provide generic upper layer security services. The parts are as follows:

1) Overview, Model and Notation.
2) Security Exchange Service Element Service Definition.
3) Security Exchange Service Element Protocol Specification.
4) Protecting Transfer Syntax Specification.
5) Security Exchange Service Element Service PICS Proforma.
6) Protecting Transfer Syntax PICS Proforma.

This Recommendation | International Standard constitutes Part 6 of the series.

Part 4 defines protecting transfer syntax for communications transfers between open systems as part of the operation of a security mechanism. To evaluate the conformance of a particular implementation, it is necessary to have a description of the capabilities and options which have been implemented. Such a description is called a Protocol Implementation Conformance Statement (PICS).

This Recommendation | International Standard includes the PICS proforma for the protecting transfer syntax specified in Part 4 and the security transformations defined in Part 1, Annex D.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – GENERIC UPPER LAYERS SECURITY: PROTECTING TRANSFER SYNTAX PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (PICS) PROFORMA

1 Scope

This Recommendation | International Standard defines a Protocol Implementation Conformance Statement (PICS) proforma for the detailed expression of the conformance requirements of ITU-T Rec. X.833 | ISO/IEC 11586-4 and Annex D of ITU-T Rec. X.830 | ISO/IEC 11586-1. This PICS proforma is in compliance with the relevant requirements, and in accordance with the relevant guidance for a PICS proforma, given in ITU-T Rec. X.291 and ISO/IEC 9646-2. Detail of the use of this proforma is provided in this Recommendation | International Standard. Implementations claiming conformance to ITU-T Rec. X.833 | ISO/IEC 11586-4 or Annex D of ITU-T Rec. X.830 | ISO/IEC 11586-1 shall complete the proforma as part of the conformance requirements. The level of detail required in the proforma exceeds that of the protocol specification by requiring details to uniquely identify the implementation and the supplier.

NOTE – PICS are related to base Recommendations and Standards and only base Recommendations and Standards. PICS structure might be expanded and refined for other documents using the base Standards (e.g. ISPICS).

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and the parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.830 (1995) | ISO/IEC 11586-1:1996, *Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation.*
- ITU-T Recommendation X.833 (1995) | ISO/IEC 11586-4:1996, *Information technology – Open Systems Interconnection – Generic upper layers security: Protecting transfer syntax specification.*
- ITU-T Recommendation X.210 (1993) | ISO/IEC 10731:1994 *Information technology – Open Systems Interconnection – Basic Reference Model: Conventions for the definition of OSI services.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- ITU-T Recommendation X.290 (1995), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – General concepts.*

  ISO/IEC 9646-1:1994, Information technology – *Open Systems Interconnection – Conformance testing methodology and framework – Part 1: General concepts.*
- ITU-T Recommendation X.291 (1995), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – Abstract test suite specification.*

  ISO/IEC 9646-2:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract Test Suite specification.*

3 Definitions

3.1 This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.290 and ISO/IEC 9646-1:

a) Protocol Implementation Conformance Statement (PICS);

b) PICS proforma;

c) Protocol Implementation extra Information for Testing (PIXIT).

4 Abbreviations

4.1 The following abbreviations used in this Recommendation | International Standard are defined in ITU-T Rec. X.290 and ISO/IEC 9646-1:

a) PICS;

b) PIXIT.

5 Conventions

This Recommendation | International Standard uses the descriptive conventions in the OSI Service Conventions, ITU-T Rec. X.210 | ISO/IEC 10731. The PICS proforma Annex A has been designed to be a self contained section of this Recommendation | International Standard, for use in testing and procurement.

6 Conformance

A conforming PICS proforma shall be technically equivalent to the ITU-T | ISO/IEC published PICS proforma and shall preserve the numbering and ordering of the items in the ITU-T | ISO/IEC PICS proforma.

A PICS which conforms to this Recommendation | International Standard shall:

a) describe an implementation which conforms to ITU-T Rec. X.833 | ISO/IEC 11586-4;

b) be a conforming PICS proforma, which has been completed in accordance with the instruction for completion given in A.1 and A.3; and

c) include the information necessary to uniquely identify both the supplier and the implementation.

Annex A[1)]

Protocol Implementation Conformance Statement (PICS) proforma for the Protecting Transfer Syntax

(This annex forms an integral part of this Recommendation | International Standard)

A.1 Notations defined for the proforma

In order to reduce the size of tables in the PICS proforma, notations have been introduced that have allowed the use of a multi-column layout, where the columns are headed 'Status', and 'Support'. The definition of each of these follows.

A.1.1 Status column

This column indicates the level of support required for conformance to ITU-T Rec. X.833 | ISO/IEC 11586-4. The values are as follows:

M Mandatory support is required.

O Optional support is permitted for conformance to ITU-T Rec. X.833 | ISO/IEC 11586-4. If implemented it must conform to the specifications and restrictions contained in ITU-T Rec. X.833 | ISO/IEC 11586-4. These restrictions may affect the optionality of other items.

n/a The item is not applicable.

c*n* The item is conditional (where *n* is the number which identifies the condition which is applicable). The definitions for the conditional statements used in this Annex are written under the tables in which they first appear.

O.*n* The item is optional, but the optionality is qualified (where *n* is the number which identifies the qualification which is applicable). The definitions for the qualified optional statements used in this Annex are written under the tables in which they first appear.

A.1.2 Support column

The 'Support' column shall be completed by the supplier or implementor to indicate the level of implementation of each feature. The proforma has been designed such that the only entries required in the 'Support' column are:

Y Yes, the feature has been implemented

N No, the feature has not been implemented

– Not applicable.

A.2 PICS numbers

Each line within the PICS proforma which requires implementation detail to be entered is numbered at the left hand edge of the line. This numbering is included as a means of uniquely identifying all possible implementation details within the PICS proforma. The need for such unique referencing has been identified by the testing bodies.

The means of referencing individual responses should be to specify the following sequence:

a) a reference to the smallest subclause enclosing the relevant item;

b) a solidus character, '/';

c) the reference number of the row in which the response appears;

d) if, and only if, more than one response occurs in the row identified by the reference number, then each possible entry is implicitly labelled a, b, c, etc., from left to right, and this letter is appended to the sequence.

[1)] **Copyright release for PICS proforma**
Users of this Recommendation | International Standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose, and may further publish the completed PICS.

A.3 Completion of the PICS

The implementor shall complete all entries in the column marked 'Support'. In certain clauses of the PICS proforma further guidance for completion may be necessary. Such guidance shall supplement the guidance given in this clause and shall have a scope restricted to the clause in which it appears. In addition, other specifically identified information shall be provided by the implementor where requested. No changes shall be made to the proforma except the completion as required. Recognizing that the level of detail required may, in some instances, exceed the space available for responses a number of responses specifically allow for the addition of appendices to the PICS.

A.4 Date of statement

Date of statement? (yy-mm-dd)

A.5 Implementation details

The supplier of the protocol implementation shall specify the information necessary to uniquely identify the implementation and the system in which it may reside. This may include details of:

a) supplier, implementation name, operating system, suitable hardware;

b) system supplier and/or client of the test laboratory that is to test the implementation;

c) information on whom to contact if there are queries concerning the content of the PICS; and

d) the relationship between this PICS and the System Conformance Statement for the System (see note).

NOTE– The System Conformance Statement is identified in ITU-T Rec. X.290 and ISO/IEC 9646-1. It contains a declaration of the layers of the Reference Model covered by the implementation to be tested.

A.6 ITU-T Rec. X.833 | ISO/IEC 11586-4 protocol details

A.6.1 ITU-T Rec. X.833 | ISO/IEC 11586-4 technical corrigenda implemented

A.7 Global statement of conformance

Are all mandatory features implemented? (Yes or no)

NOTE – If a positive response is not given to this box, then the implementation does not conform to ITU-T Rec. X.833 | ISO/IEC 11586-4.

A.8 Supported syntax structures

	Syntax structure	Sending		Receiving		Reference	Comment
		Status	Support	Status	Support		
A.8/1	First PDV explicit	O		O	Part 4 5.4, 6		
A.8/2	First PDV external	O		O	Part 4 5.4, 6		
A.8/3	Subsequent PDV	O		O	Part 4 5.4, 6		

A.9 Supported PDV fields

A.9.1 First PDV explicit

	Field	Sending		Receiving	
		Status	Support	Status	Support
A.9.1/1	Transformation Id	c1		c1	
A.9.1/2	Static Unprotected parameters	c2		c2	
A.9.1/3	Dynamic Unprotected parameters	c2		c2	
A.9.1/4	Xformed Data	c1		c1	
	c1: if [A.8/1] then M else n/a c2: if [A.8/1] then O else n/a				

A.9.2 First PDV external

	Field	Sending		Receiving	
		Status	Support	Status	Support
A.9.2/1	External Context Id	c3		c3	
A.9.2/2	Dynamic Unprotected parameters	c4		c4	
A.9.2/3	Xformed Data	c3		c3	
	c3: if [A.8/2] then M else n/a c4: if [A.8/2] then O else n/a				

A.9.3 Subsequent PDV

	Field	Sending		Receiving	
		Status	Support	Status	Support
A.9.3/1	Dynamic Unprotected parameters	c6		c6	
A.9.3/2	Xformed Data	c5		c5	
	c5: if [A.8/3] then M else n/a c6: if [A.8/3] then O else n/a				

A.10 Establishment of encoding for Protecting Transfer Syntax

		Ref	Status	Support
A.10/1	Specific encoding / decoding rules implied	Part 4 5.2 a)	O	
A.10/2	Specific encoding / decoding rules not implied	Part 4 5.2 b)	O	

A.11 Security transformations

A.11.1 Security Transformations Supported

		Ref	Status	Support
A.11.1/1	Directory Encrypted Transformation	Part 1 Annex D1	O	
A.11.1/2	Directory Signed Transformation	Part 1 Annex D2	O	
A.11.1/3	Directory Signature Transformation	Part 1 Annex D3	O	
A.11.1/4	GULS Signed Transformation	Part 1 Annex D4	O	
A.11.1/5	GULS Signature Transformation	Part 1 Annex D5	O	

A.11.2 Directory Encrypted Transformation

A.11.2.1 Parameters

No parameters defined.

A.11.2.2 Other information

		Status	Support	
A.11.2.2/1	Associated Protection Mapping	c7	ASN.1 name	
A.11.2.2/2	Initial Encoding Rules	c7	BER / DER / Canonical Other	
	c7: if [A.11.1/1] then O else n/a			

A.11.3 Directory Signed Transformation

A.11.3.1 Parameters

		Sending		Receiving	
		Status	Support	Status	Support
A.11.3.1/1	(data) to be signed	c8		c8	
A.11.3.1/2	Algorithm	c9		c9	
A.11.3.1/3	Other algorithm specific parameters	c9		c9	
A.11.3.1/4	Enciphered Hash	c8		c8	
	c8: if [A.9.1/2] then M else n/a c9: if [A.9.1/2] then O else n/a				

A.11.3.2 Other information

		Status	Support	
A.11.3.2/1	Associated Protection Mapping	c9	ASN.1 name	
A.11.3.2/1	Initial Encoding Rules	c9	DER	

A.11.4 Directory Signature Transformation

A.11.4.1 Parameters

		Sending		Receiving	
		Status	Support	Status	Support
A.11.4.1/1	Algorithm	c10		c10	
A.11.4.1/2	Other algorithm specific parameters	c10		c10	
A.11.4.1/3	Enciphered Hash	c11		c11	

c10: if [A.11.1/3] then O else n/a
c11: if [A.11.1/3] then M else n/a

A.11.4.2 Other information

		Status	Support	
A.11.4.2/1	Associated Protection Mapping	c10	ASN.1 name	
A.11.4.2/2	Initial Encoding Rules	c10	DER	

A.11.5 GULS Signed Transformation

A.11.5.1 Parameters

		Sending		Receiving	
		Status	Support	Status	Support
A.11.5.1/1	Unprotected item	c12		c12	
A.11.5.1/2	Initial Encoding Rules	c13		c13	
A.11.5.1/3	Sign or Seal Algorithm	c13		c13	
A.11.5.1/4	Hash Algorithm	c13		c13	
A.11.5.1/5	Key Information	c13		c13	
A.11.5.1/6	Appendix	c12		c12	

c12: if [A.11.1/4] then M else n/a
c13: if [A.11.1/4] then O else n/a

A.11.5.2 Other information

		Status	Support	
A.11.5.2/1	Associated Protection Mapping	c13	ASN.1 name	
A.11.5.2/2	Initial Encoding Rules	c13	Canonical If N, specify	
A.11.5.2/3	Direct encoding (see Part 1, 8.1)	c14	Supported	
A.11.5.2/4	Embedded encoding (see Part 1, 8.1)	c14	Supported	
A.11.5.2/5	Protecting transfer syntax (see Part 4, clause 9)	c15	GULS General If N, specify	
	c14: if not [A.11.1/4] then n/a else either Direct or embedded encoding must be selected c15: if not [A.11.1] then n/a else if [A.11.5.2/3] then GULS General is m else o			

A.11.6 GULS signature transformation

A.11.6.1 Parameters

		Sending		Receiving	
		Status	Support	Status	Support
A.11.6.1/1	Initial Encoding Rules	c16		c16	
A.11.6.1/2	Sign or Seal Algorithm	c16		c16	
A.11.6.1/3	Hash Algorithm	c16		c16	
A.11.6.1/4	Key Information	c16		c16	
A.11.6.1/5	Appendix	c17		c17	
	c16: if [A.11.1/5] then O else n/a c17: if [A.11.1/5] then M else n/a				

A.11.6.2 Other information

		Status	Support	
A.11.6.2/1	Associated Protection Mapping	c16	ASN.1 name	
A.11.6.2/2	Initial Encoding Rules	c16	Canonical If N, specify	
A.11.6.2/3	Direct encoding (see Part 1, 8.1)	c18	Supported	
A.11.6.2/4	Embedded encoding (see Part 1, 8.1)	c18	Supported	
A.11.6.2/5	Protecting transfer syntax (see Part 4, clause 9)	c19	GULS General If N, specify	
	c18: if not [A.11.1/5] then n/a else either Direct or embedded encoding must be selected c19: if not [A.11.1/5] then n/a else if [A.11.5.2/3] then GULS General is M else O			

ICS 35.100.01

Descriptors: data processing, information interchange, network interconnection, open systems interconnection, communication procedure, security techniques, protocols, implementation.

Price based on 9 pages